Fusing Open Source Intelligence and Handheld Situational Awareness

Benghazi Case Study

Jeff Boleng, PhD
Marc Novakouski
Gene Cahill
Soumya Simanta
Edwin Morris

jlboleng@sei.cmu.edu

Software Engineering Institute
Carnegie Mellon University®

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 OCT 2014	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Fusing Open Source Intelligence and Handheld Situational Awareness - Benghazi Case Study	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Jeffrey L. Boleng	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**22**	

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0001694

Overview

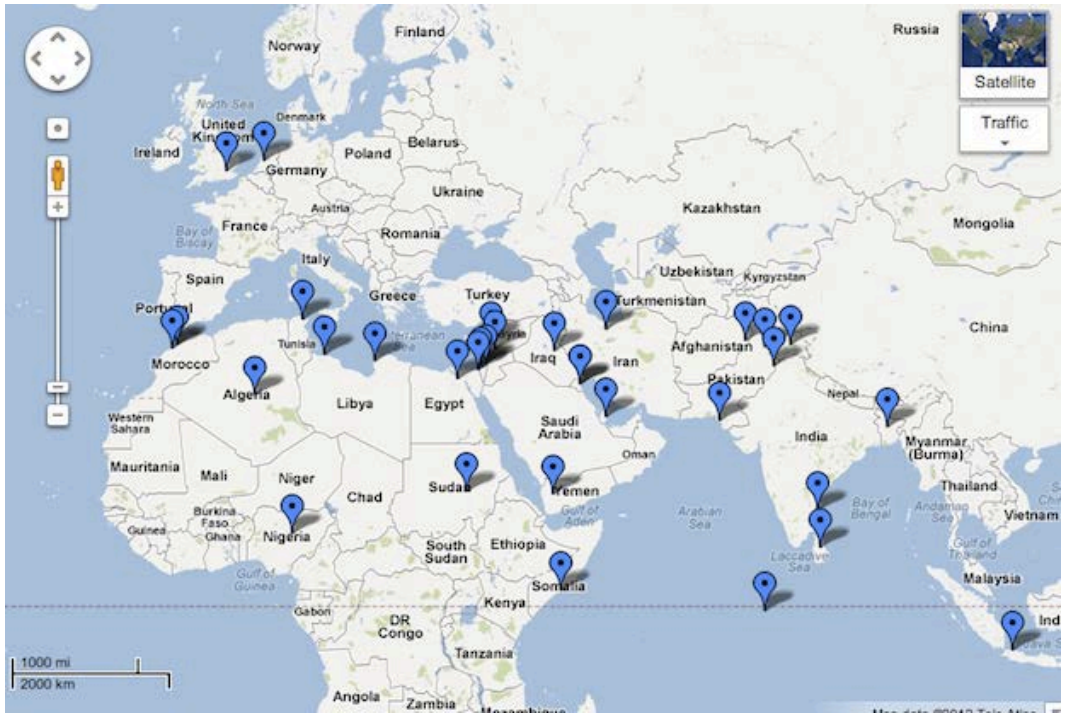
- Background
- Scenario Overview
- Edge Analytics
- Information Superiority to the Edge
- Findings
- Conclusions

Background

- **Request by DoD stakeholders**
  - Develop prototype from existing technology to demonstrate mobile handheld situational awareness (SA) to aid US personnel in foreign countries
- **Combine two ongoing research prototypes**
  - Information Superiority to the Edge (ISE)
    - Group context aware middleware and handheld SA
  - Edge Analytics
    - Streaming data analysis to support rapid Intelligence Preparation of the Battlespace (IPB)
- **Link OSINT to mobile SA**

Background

- **Between September 11 and 17, 2012, diplomatic missions in the Middle East, Asia, and Europe were subject to protests and violent attacks in response to an inflammatory video, *Innocence of Muslims*.**



Cairo: Reaction to YouTube Trailer

11 Sep 2012 @ 5pm:
About 3,000 demonstrators assemble outside the American Embassy in Cairo.

About a dozen men scaled the walls and tore down the US flag, replacing it with the black Islamist flag bearing the inscription Shahada ("There is no god but God and Muhammad is the messenger of God.")

Cairo Demonstration Timeline

Soliman_solo @Soliman_solo Tue Sep 11 14:57:10 -0400 2012
Al-Qaeda flags flapping in the Mohamed Mahmoud Street # Egypt # _ U.S. Embassy http://t.co/Tw0q9rb2

Tahrir_now @Tahrir_now Tue Sep 11 12:49:47 -0400 2012
Today's demonstration in front of the U.S. Embassy in Cairo at 5 to object to insult the Prophet Muhammad peace be upon him by some of the ... http://t.co/hnZJUMnE

7o0okaaa @7o0okaaa Tue Sep 11 15:54:29 -0400 2012
3 youth clothed in T-shirt Martyrs Oltras Ahlawy Perfau aware of "No God but God and Mohammed is the Messenger of Allah" place American flag http://t.co/cp1ZOB7r

RawSmackdownTNA @RawSmackdownTNA Tue Sep 11 19:42:27 -0400 2012
Protesters angered by US film "insulting to Prophet Muhammad" breach wall of US embassy in #Cairo, #Egypt via @BBCBreaking

Before Demonstration

During Demonstration

Attack on Embassy

After Demonstration

Benghazi: Reaction

11 Sep 2012 @ 10:40 pm: Large numbers of armed men shouting "Allahu Akbar" descend on the compound from multiple directions lobbing grenades over the wall followed by automatic weapons fire and RPG's. The assailants are backed by truck-mounted artillery and anti-aircraft machine guns.

Note

The following participants and events are notional and were created to explore what might have been possible by integrating social media information (OSINT) with traditional intelligence combined with improved mobile situational awareness and communications.

Preparation

- **Analyzed over 1.2M tweets from the 2 weeks surrounding the Benghazi and Cairo events**
- **Geographically centered on Benghazi and Cairo**
- **Numerous keywords included in search**
- **Included English (≈60%) and machine translated Arabic tweets (≈40%)**
  - Not a perfect translation, but suitable for machine learning algorithmic analysis
- **Integrated two existing research prototypes to enable data sharing**

Scenario Overview

Several notional people that could have been in Benghazi at the time of the attack

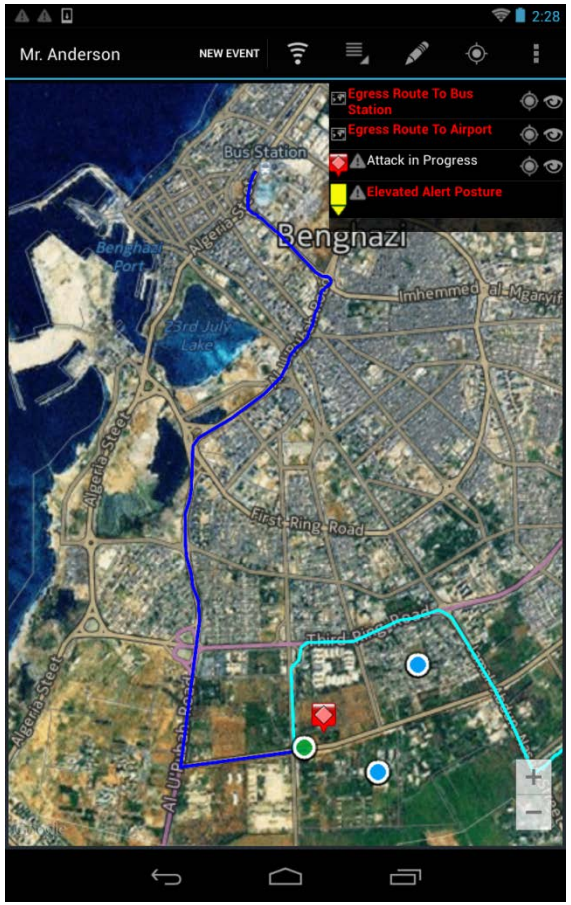
- (BT) Business Traveler – a US citizen travelling and operating in Benghazi strictly for business purposes.
- (CE) Consulate Employee – a US consulate employee stationed at the diplomatic mission in Benghazi, but not present on the compound at the start of the attack.
- (SO) Special Operator – multiple US Special Operations personnel on a variety of missions in Benghazi at the outset of the attack.
- (QRF) Quick Reaction Force – the members of the quick reaction force that deployed from the CIA compound near the diplomatic mission after the attack began.
- (C2) Command and Control – a command and control element at the CIA compound that would have been monitoring OSINT and other sources of intelligence before the attack and coordinating response and C2 of the various other actors as events unfolded.

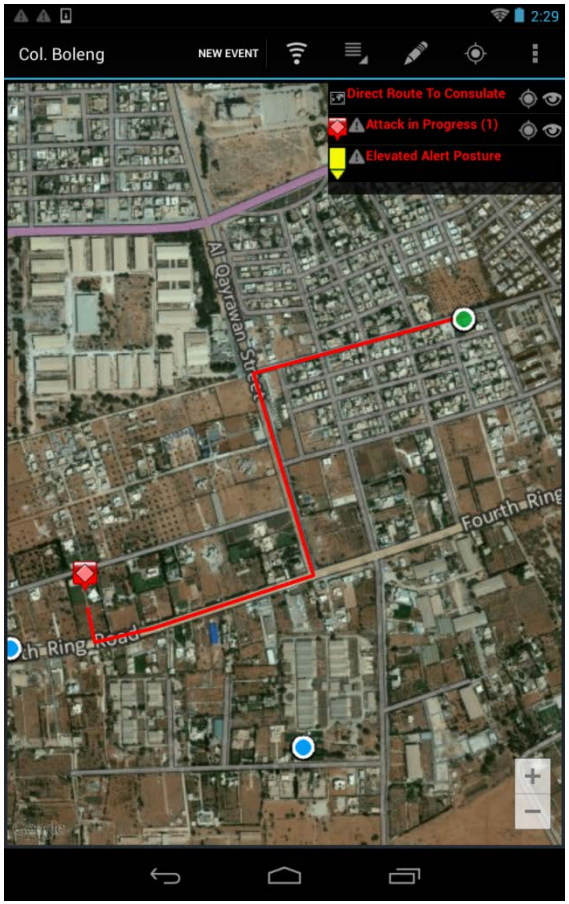
Scenario Overview

- Scenario begins by monitoring social media and other channels in the days prior to the release of “Innocence of Muslims” on YouTube (11 Sep 12)
- Large social media activity calling for a demonstration at the US Embassy in Cairo
- (6:00 pm) Data and imagery regarding the Cairo breach are shared with the Benghazi C2 Intel element
- (9:40 pm) Attack on diplomatic mission in Benghazi begins
  - Alarm sounds and is noticed by the C2 element at the CIA Annex
  - Attack in progress message sent to all users on mobile device
  - Rules provide contextually relevant information to each user

Screen shot examples

BT is instructed to leave the city, egress routes to airport and bus station avoiding the attack are presented

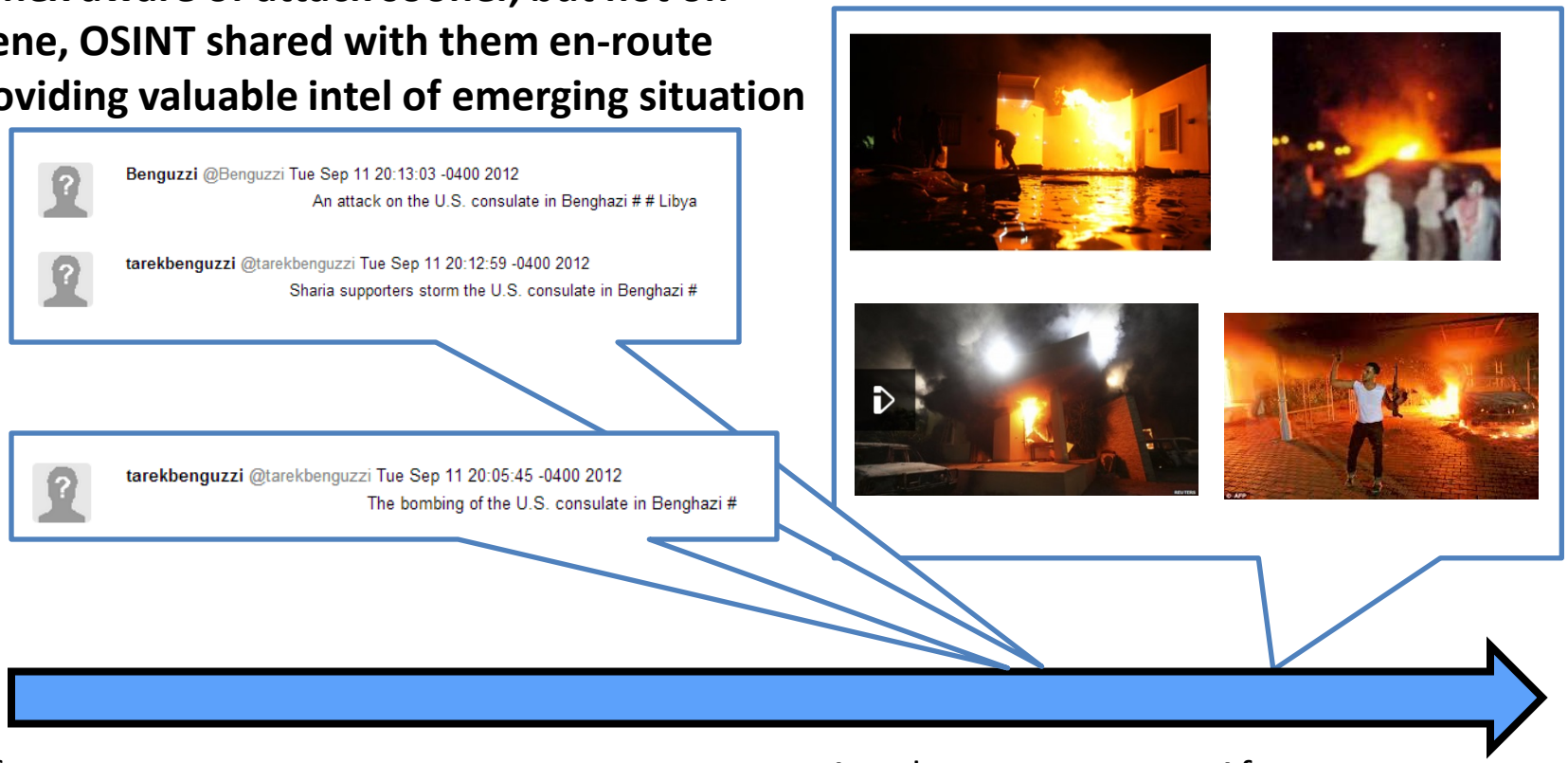




SO personnel are notified and allowed to respond in support or continue on current mission, routing to attack is presented

Benghazi Timeline

- **Tweets and social media artifacts of attack appear 20-25 minutes after the outset**
- **Annex aware of attack sooner, but not on scene, OSINT shared with them en-route providing valuable intel of emerging situation**



Remainder of the scenario

- Scenario continues with SO personnel responding and assisting QRF
- SO provides over watch and intel to QRF before they arrive at consulate
  - Images, video, approach routes, and map annotations all provided
- Consulate employee is routed successfully around roadblock and is extracted by QRF
- Real time location of all personnel appropriately shared based on need to know
- Scenario concludes with coordinated extraction of all personnel via the airport similar to Senate report
- Full scenario details sensitive

Edge Analytics: What we learned from twitter

- **Cairo**
  - Demonstration was well planned. Lots of trending social media before hand
  - No evidence of embassy wall breach planned in the Cairo tweets
  - Breach appears to have been opportunistic but demonstration was well planned
- **Benghazi**
  - No evidence of planning for demonstration OR attack in Benghazi – Twitter silent
  - About 22 minutes after the attack began Twitter begins to trend
  - Initial traditional media reports say that the attack was the result of a demonstration
  - Social media totally refutes this
  - Lack of strong trending initially from the Benghazi attack can be informative
    - No attempt to rally protesters may hint that it was not and never was a protest
    - Knowing it was not a protest may allow responding forces to operate differently
      - *fewer concerns about innocents caught up in attack*

Value of OSINT

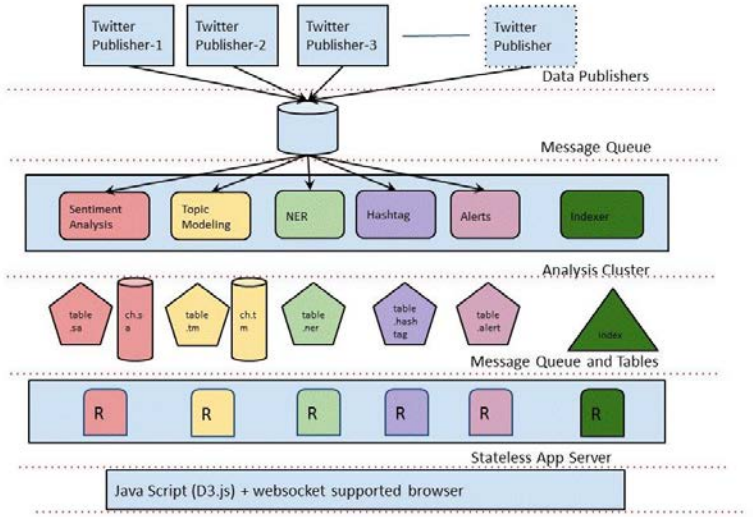
- **Forensic Analysis**
  - apply data mining techniques to historical data
- **Reactive Intelligence**
  - provides situational awareness to reacting teams such that they are informed of emerging events and can react to those events
- **Predictive Intelligent**
  - that allows reacting teams to prepare for an event that has a relatively high likelihood of occurring
- **Preventative Intelligence**
  - that allows reacting teams to head off certain events by providing information that reduces the likelihood of these events

Additional Findings

- **Machine Language Translation (MLT) of foreign languages is sufficient for many uses**
- **Contextual delivery of information by role and task (profile) is effective**
  - Reduces information clutter and cognitive load
  - Facilitates information sharing and timeliness
- **Real time analysis of streaming data**
  - Not appropriate to find the “needle in the haystack”
    - Might be possible during forensic analysis
  - Patterns and signatures of events stand out
  - Sophisticated adversaries do not use social media
  - However, field experiments show significant events that can threaten public safety trend on twitter **before** they occur

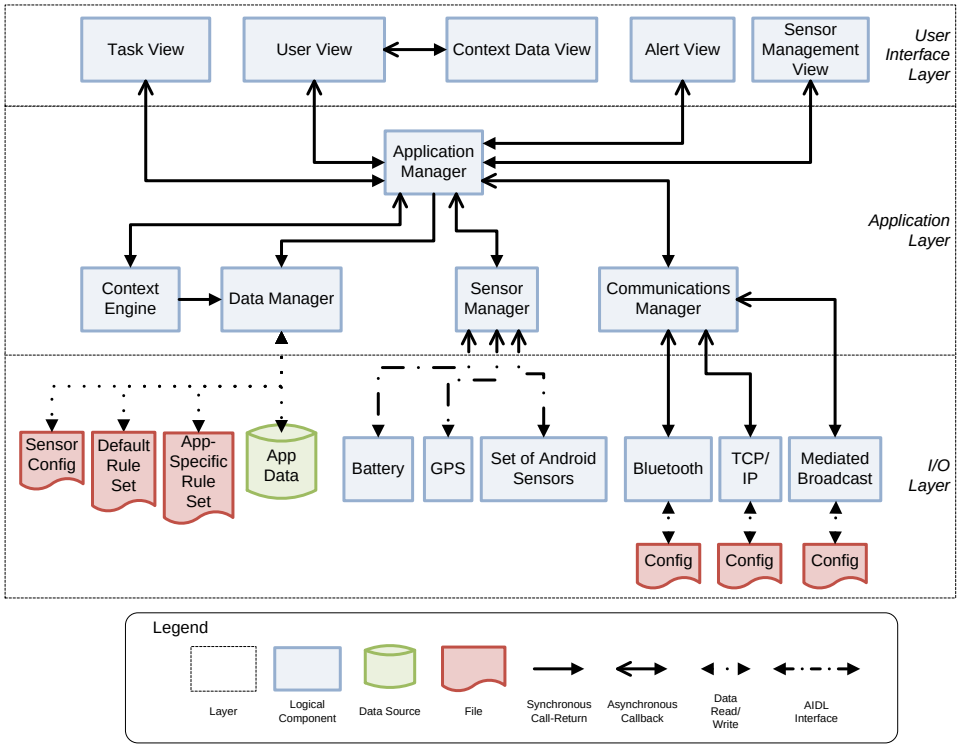
Edge Analytics

- Scalable architecture for real time streaming data
- Currently focused on Twitter
- Used in numerous field experiments
  - CreationFest 2013 and 2014
  - Little League World Series
  - Wireless Emergency Alert Service
  - MIT LL Next-Generation Incident Command System
- Pluggable analysis engines
- Accessible via web browser
- FY15 integrating/fusing non-textual information streams



Information Superiority to the Edge (ISE)

- Group context aware architecture and middleware to facilitate effective SA and information sharing
- Expanded context model to include mission, role, and task
- Mission tailor able rules engine is the heart of the context engine
- Android client to demonstrate value of group collaboration via handhelds
- Integrated Delay Tolerant Networking (DTN) protocols and meta-data extensions for effective use in DIL environments



Future Work

- **Edge Analytics**
  - Improved multi-lingual capabilities
  - Geo-inferencing (implemented)
  - Social network analysis (implemented)
  - Semantic evaluation of keyword combinations (partially implemented)
  - Include alternative data stream formats (FY15)
  - Credibility evaluation of social media data (FY15)

Information Superiority to the Edge

- DTN meta-data extension support (implemented)
- Multi-radio channel DTN routing (implemented)
- Extend mission/role/task model for automated in mission adaptation

- **For more information, contact:**

Jeff Boleng
jlboleng@sei.cmu.edu
412-268-9595